IN THE CLAIMS

1. – 36. Canceled.

37. (Currently Amended) A method of validating the integrity of a data packet for stream cipher out-of-synchronization detection, the method comprising:

decrypting a data packet containing a checksum and a payload, the checksum included in a header of the data packet and based upon the payload, the decrypting accomplished using a forward cipher key;

extracting the checksum from the decrypted data packet;

calculating a calculated checksum for the data packet, the calculated checksum generated by a checksum generator based on the payload of the data packet;

comparing the checksum extracted from the decrypted data packet with the calculated checksum at a checksum validation engine; and

detecting a loss of stream cipher synchronization if the calculated checksum does not match the checksum extracted from the decrypted data packet.

38. (Previously presented) The method of claim 37, wherein detecting a loss of stream cipher synchronization if the calculated checksum does not match the checksum extracted from the decrypted data packet further comprises:

a network layer of a protocol stack detecting the loss of stream cipher synchronization when the calculated checksum does not match the checksum extracted from the decrypted data packet.

39. (Previously presented) The method of claim 37, further comprising:

comparing the calculated checksum and the checksum extracted from the decrypted data packet both for a network layer data payload.

40. (Previously presented) The method of claim 37, further comprising:

re-synchronizing a stream cipher with a transmitter of the encrypted data packet if the calculated checksum does not match the checksum extracted from the decrypted data packet.

41. Canceled.

42. Canceled.